SECURELINK

How your vendor access management tools are putting your company at risk

Nearly two-thirds of all companies have experienced a data breach due to third-party network access. Your company could be next.

If third parties are accessing your network, whether you're using a VPN, a vendor-supplied support tool, or a Privileged Access Management (PAM) solution to manage vendor network access, the limitations of those tools leave you vulnerable to breaches. But you can't manage risks that you don't know you have.

While you grant your employees complete network access, your vendors should be on a need-to-know basis, and should only be able to access the information and systems they truly need in order to be an effective third-party partner. And to ensure third-party secure access, there's a lot you need to know:

Chances are you may not collect or monitor some or all of this information. And what you don't know can likely lead to a breach that will hurt you, your business, and your customers.

» How many vendors are accessing your network and systems?

» Which individuals within a third-party organization are accessing those resources?

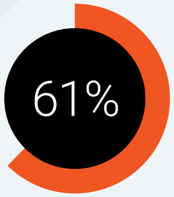
» Are the individuals accessing your network still employed by the third-party vendor?

» What information do your third-party vendors need to access on your network and systems?

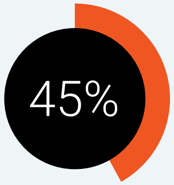
» Can you restrict network access to only the information required—or do you grant access to all of your systems?

» When did your third parties access your network—and what have they accessed, modified, or deleted?

» Can you see when your third-party vendors accessed your network and systems—and what information they accessed, modified, or deleted?



Of all companies have experienced a data breach caused by a third-party vendor.



And 45% have experienced a third-party vendor breach in the last 12 months.

Source: Data Risk in the Third-Party Ecosystem, Ponemon Institute LLC, "Third Annual Research Report"

What are the limitations of your current vendor access management tools?

Where are the gaps in the current tools you may be using for third-party vendor access—and why do they increase the risk of a breach?

VPN

If you're using VPNs, you probably think your company data and network are safe. But nothing could be further from the truth. VPNs are great for managing remote employee access, but fall short when it comes to third-party vendor network access:

All or nothing. VPNs provide access to your entire network, instead of specific systems—great for employees but not for vendors whose access should be limited.

Complexity and cost. VPNs are costly. It takes time to provision and secure, revoke provisioning, control who is accessing what and when on your network, and provide technical support to users.

Compromised Active Directory. VPN access is granted based on members in the company's Active Directory, which is typically restricted to employees. You'll need to merge vendors in with employees, weakening security by providing vendors with privileged accounts that are frequently targeted due to their broad network access.

No individual user visibility. You don't have any way of knowing who is specifically accessing your network and if they are valid employees.

PRIVILEGED ACCESS MANAGEMENT

If you are using a PAM platform to manage vendors, vendors are treated like employees, which means they will get more rights than required to do their job. PAM platforms do provide some improvements over enterprise VPNs for privileged access, but there are still limitations.

No remote access. Since most of your vendors are external, you'll need to also deploy a VPN to enable access to your network from outside your firewall, adding to solution complexity—and increasing your costs.

Employee rights for vendors. You'll need to manage vendor users the same as employee users, which provides vendors with more network access than required to get their job done.

VENDOR-SUPPLIED SUPPORT TOOLS

If you give vendors the responsibility for network access and allow them to provide their own tools, then cost, time, and security remain issues.

Complexity. Every vendor can have a different tool with a different set of security features they choose to activate, forcing you to manage multiple technologies—a very time-consuming and costly effort.

No access control. It is difficult, if not impossible, to constrain network access to only the needed network resources.

Credential security. You have no control over the security of the actual credentials. So the keys to your network could be in a file on a user's laptop with an obvious name or on a sticky note on a desk, where it is visible to all who pass by.

Vendor Privileged Access Management

A simple, secure way to manage remote access for your third-party vendors

Until now, third-party vendor network access has been administered by tools designed for secure employee access—like trying to put a round peg in a square hole. In order to better meet the unique requirements needed to enable secure and easy-to-manage third-party vendor network access, a new category of tools has emerged: Vendor Privileged Access Management (VPAM).

Where PAM is designed for employees, VPAM is designed with the unique needs of third parties in mind, providing the big four features missing from all of today's network access management solutions.

THE VPAM BIG 4

Least privileged access

Easily provide third-party vendors with access only to those network and system resources needed to get the job done.

Authenticate each vendor user

Provide credentials for each user at each vendor, rather than one set of credentials for all workers at a given company.

Detailed audit for every user

Now you'll know exactly what third-party users are doing while they are on your network and can record every keystroke and all commands entered. You'll have all the information you need to ensure compliance and support investigations into breaches or security incidents.

Centralized management

You need a centralized command center that will track all users and their credentials, correlate audit trails, and enable easy configuration of which network resources each user can access.

For more information, or for a personalized ROI calculation showing how much you will save every year while increasing the security and manageability of third-party vendor network access, please visit **securelink.com** or call us at **1.888.897.4498.**

About SecureLink

SecureLink is the leader in managing secure vendor privileged access and remote support for both highly regulated enterprise organizations and technology vendors. More than 30,000 organizations across multiple industries including healthcare, financial services, legal, gaming, and retail rely on SecureLink's secure, purpose-built platform. SecureLink is headquartered in Austin, Texas.

securelink.com | 888.897.4498 | contact@securelink.com